NIFIS Nationale Initiative für Informations- und Internet-Sicherheit

advice
05/2008

Liebe NIFIS-Mitglieder,

sehr geehrte Interessenten und Förderer,

die letzten Wochen haben gezeigt, welche Konsequenzen eine defizitäre Informations-Sicherheit für das Image eines Unternehmens haben kann. Trotz eines hohen Fokus auf die Informations-Sicherheit und der Bereitstellung umfangreicher personeller und finanzieller Ressourcen ist es der Deutschen Telekom nicht gelungen, das Ausspähen von Kundendaten zu verhindern.

Eine zunehmende Digitalisierung und noch stärkere Vernetzung zwingt Unternehmen dazu, in Sicherheitsfragen auf verschiedenen Ebenen zu agieren. Grundlegend sind Prozesse, die zunächst Berechtigungen und Datenzugriffe für Mitarbeiter und Zulieferer – auch Call Center – regeln. Die Berechtigungen selbst müssen regelmäßig überprüft, angepasst und mithilfe von technischen Lösungen umgesetzt werden, die die Überwachung und Protokollierung regeln. Um eine ganzheitliche Sicherheit herstellen zu können, werden oftmals mehrere Speziallösungen parallel eingesetzt. Diese Lösungen können ihre volle Wirkung aber nur dann entfalten und für eine lückenlose sowie nachhaltige Sicherheit sorgen, wenn auch übergeordnete Managementprozesse etabliert und gelebt werden.

Genau an dieser Stelle positioniert sich NIFIS. Im Dialog mit unseren Mitgliedern möchten wir Ihnen dabei helfen, durch die Verzahnung verschiedener technischer Lösungen mit entsprechenden Prozessen ein dem Schutzbedarf Ihres Unternehmens entsprechendes Sicherheitsniveau zu erreichen.

Ich wünsche Ihnen viel Spaß beim Lesen dieser Ausgabe von NIFIS advice

Peter Knapp
Vorstandsvorsitzender

HIGHLIGHTS

NIFIS inside

NIFIS reagiert auf Datenschutzskandale

Meldungen über Datenschutzverletzungen sind mittlerweile an der Tagesordnung. Ob Telekom, Klassenlotterie, Meldeämter oder auch die DAK – alle Betroffenen versichern, dass sie sich an Gesetz und Recht halten und keine Datenübermittlung außerhalb des geltenden Rechts und ohne Einwilligung der Betroffenen erfolge oder dass sie Opfer eines kriminellen Datenraubs wurden.

NIFIS reagiert auf die jüngsten Datenmissbrauchskandale und empfiehlt Unternehmen und Organisationen das eigens entwickelte NIFIS-Siegel als erste einfache Maßnahme zur Überprüfung und Erhöhung des eigenen Sicherheitsstandards. Durch den Selbstaudit können Unternehmen eigene Sicherheitslücken erkennen und durch entsprechende Folgemaßnahmen schließen.

Bundesjustizministerin Brigitte Zypries forderte angesichts der aktuellen Datenmissbrauchsfälle eine Überprüfung des gesetzlich festgeschriebenen Datenschutzes. Doch sollte nach Einschätzung von NIFIS kein kurzfristiger Aktionismus betrieben, sondern konkrete und nachhaltige Maßnahmen zur Verbesserung des Datenschutzes initiiert und bereits eingeleitete Maßnahmen weiterentwickelt werden. Hierzu könnte auch die Fortführung der gesetzlichen Initiative zum Bundesdatenschutzauditgesetz beitragen. In ihrer ersten Stellungnahme begrüßte NIFIS diese Initiative, riet aber beim Entwurf des Gesetzes der Bundesregierung zu Nachbesserungen. ❑

Expertenforum Datenschutz tagt

Am 15. Oktober findet ab 14 Uhr die vierte Sitzung des NIFIS-Expertenforums Datenschutz in Frankfurt am Main statt, zu der NIFIS alle Interessierten und Mitglieder herzlich einlädt.

Nach den Vorarbeiten der Untergruppe Marketing wird sich das Expertenforum unter dem Oberthema „Schaffung von Awareness“ zunächst wiederum mit der Erstellung eines E-Learning-Tools für Geschäftsführer und Entscheidungsträger in Unternehmen beschäftigen. Wie bereits besprochen, soll dieses Tool dem ►

Nutzer die Möglichkeit geben, sich auf interessante und attraktive Weise mit dem wichtigen Thema „Einhaltung und Umsetzung der Bestimmungen des Datenschutzrechts in der täglichen Arbeit“ vertraut zu machen. Ziel ist es, auf Basis der bisherigen Arbeit einen deutlichen Schritt nach vorn zu unternehmen.

Ein weiteres Projekt des Expertenforums Datenschutz ist die Entwicklung eines Workshops, mit dem der konkrete Bedarf eines Unternehmens im Bereich Datenschutz schnell ermittelt werden kann. Durch verschiedene Skandale ist der Datenschutz in letzter Zeit wieder in den Blickpunkt der Öffentlichkeit und auch des Gesetzgebers geraten. Im Expertenforum Datenschutz wird daher auch die von Seiten des Gesetzgebers geplante Überarbeitung des Bundesdatenschutzgesetzes diskutiert und gemeinsam überlegt, ob und wie von NIFIS zu diesem Themenkomplex Stellung genommen und die Sichtweise der Wirtschaft eingebracht werden soll.

Dr. Thomas Lapp, der Leiter des NIFIS-Expertenforums Datenschutz, möchte gerne das für Experten ausgeschriebene Forum für Mitglieder, die weniger mit der Materie Datenschutz als solche vertraut sind, zugänglich machen. Als „Selbsthilfeorganisation der Wirtschaft“ möchte NIFIS auch das Thema Datenschutz im gegenseitigen Erfahrungsaustausch von der Wirtschaft für die Wirtschaft den Mitgliedsunternehmen nahebringen.

Die Anmeldung zur Sitzung ist über nifis@nifs.de möglich. Wir bitten um Mitteilung bis 7. Oktober, die Teilnahme ist **kostenfrei**. ❑

NIFIS auf dem EDV-Gerichtstag

Vom 17. bis zum 19. September fand dieses Jahr unter Beteiligung von NIFIS der EDV-Gerichtstag in Saarbrücken statt. Zum 17. Mal trafen sich Experten und Interessierte der Bereiche Informatik und Recht zu einem regen Informations-Austausch innerhalb verschiedener Arbeitskreise. NIFIS-Vorstand Mathias Gärtner stellte in einem Vortrag die Arbeit der Initiative im Bereich Internet- und Informations-Sicherheit vor. Anschließend ging er näher auf aktuelle Bedrohungen für die Informations-Systeme von mittelständischen Unternehmen ein. Die Anzahl von Schadprogrammen sowie die Summe der Schwachstellen in IT-Produkten verdoppele sich mindestens jährlich. Fast jede zehnte E-Mail sei mit Malware wie Viren oder Würmern verseucht, mehr als 90 Prozent aller E-Mails weltweit seien Spam.

Gärtner führte deutlich vor Augen, dass trotz der stetig steigenden Risiken für die IT der mittelständischen Unternehmen, diese nicht ausreichend in geeignete Schutzmaßnahmen investieren. Er betonte, dass NIFIS es als Aufgabe sehe, die IT-Verantwortlichen und die Geschäftsführung für diese Problematik zu sensibilisieren. ❑

Prof. Pausch & Partner erhält NIFIS-Siegel

Das Sachverständigenbüro Prof. Pausch & Partner darf für ein Jahr das NIFIS-Siegel führen und damit seinen hohen Sicherheitsstandard gegenüber Presse, Kunden und Geschäftspartnern belegen.

„Wir haben uns für die Bewerbung um ein NIFIS-Siegel entschieden, weil wir damit eine externe Sicht auf unsere IT-Sicherheit bekommen haben. Im Nachgang der Bewertung kannten wir dank NIFIS unsere Schwachstellen und konnten diese teilweise auch durch einfachste Maßnahmen, wie zum Beispiel den Kauf von zusätzlichen Brandmeldern, abstellen. Natürlich werden wir die erfolgreiche Bewertung auf unserer Webseite veröffentlichen, um somit unseren Qualitätsstandard zu dokumentieren“, berichtet Dr. Simone Richter von Prof. Pausch & Partner.

Für NIFIS-Mitglieder ist der Erwerb des speziell für die mittelständische Wirtschaft entwickelten Siegels ebenso wie die Rezertifizierung **kostenfrei**. Für Nicht-Mitglieder kostet das Audit 150 Euro. ❑

NIFIS beruft AK Validierung ein

Informations-Sicherheit ist mittlerweile für die meisten Unternehmen und Organisationen keine Frage mehr. Das „Wie?“ und „Was?“ stellt für viele jedoch nach wie vor eine große Herausforderung dar. Idealerweise soll Informations-Sicherheit nicht nur zum Schutz vor den allgegenwärtigen Gefahren und möglichen Angriffen dienen, sondern auch dazu beitragen, das Unternehmen besser zu positionieren. Der NIFIS-Arbeitskreis Validierung wird diese Fragen und Themen aufgreifen und umfassend bearbeiten.

Die Teilnehmer wollen gemeinsam Hilfsmittel erarbeiten, die eine pragmatische, stufenweise Vorgehensweise erlauben, und diese den Mitgliedern zur Verfügung stellen. Zudem ist es Ziel, das NIFIS-Siegel weiterzuentwickeln und dessen Ansehen als ein aussagekräftiges, valides Markenzeichen weiter zu stärken. Die Treffen des AKs dienen natürlich auch dem Informationsaustausch zu aktuellen Bedrohungen, Sicherheitsvorfällen, Richtlinien und Standards.

Die erste Sitzung des AK Validierung findet am 3. Dezember von 10 bis 15 Uhr in Frankfurt statt. Die Leitung übernimmt Ingrid Dubois, Geschäftsführerin der dubois it-consulting gmbh. Sie ist lizenziert als Auditorin für Informations-Sicherheit (ISO/IEC 27001, ISO 27001 auf der Basis von IT-Grundschutz) und für Business Continuity (BS 25999). Im Laufe ihrer beruflichen Entwicklung hat sie in der Anwendungsentwicklung, Systemadministration und als Beraterin in verschiedensten Projekten mitgewirkt.

Alle Mitglieder und Interessenten sind herzlich eingeladen, an der Sitzung des AKs teilzunehmen. Die Teilnahme ist **kostenfrei**. Bitte melden Sie sich bis zum 15. November bei nifis@nifis.de an. Für Rückfragen steht Barbara Saul telefonisch unter 069/40809370 oder per Mail (marketing@nifis.de) gerne zur Verfügung. ❑

Veranstaltungstipps

NIFIS-Vortrag bei VO.IP Germany

Ist unsere Kommunikation fit für die Herausforderungen der nächsten Generation? Dieser Frage geht die VO.IP Germany am 28. und 29. Oktober in Frankfurt am Main nach. Die Kongressmesse für Voice- und IP-Kommunikation bietet dank praktischer Vorführungen und durch Vorträge namhafter Vertreter vornehmlich aus der Wirtschaft, aber auch von Politik, Regulierung und Verbänden, einen umfassenden Überblick über den Entwicklungsstand, die Zusammenhänge und Auswirkungen des Zusammenwachsens von Sprache und Daten, Netzen und Systemen in Unternehmen.

NIFIS-Vorstand Dr. Thomas Lapp wird am ersten Tag im Themenblock „Zukunft“ über rechtliche Aspekte bei den Next Generation Networks referieren.

Die Teilnahme an einem Kongresstag kostet 249 Euro, an beiden Tagen 449 Euro plus MwSt.. ❑

Praxisforum Identity Management

Jetzt schon vormerken:
Am 29. Januar 2009 veranstaltet NIFIS in Kooperation mit der Landesinitiative secure-it.nrw das Praxisforum Identity Management (IM). Im Mittelpunkt stehen Lösungsmöglichkeiten und Umsetzungstipps für die Einführung von Identity Management.

Renommierte Referenten wie Jürgen Skirde, Abteilungsleiter IT-Infrastruktur bei der RAG AG und Dr. Horst A. Walther, Leiter des NIFIS-Expertenforums IM und Geschäftsführer der SiG Software Integration GmbH, gewähren einen interessanten Einblick in die Arbeit mit Identity Management. NIFIS-Vorstand Dr. Thomas Lapp erläutert die rechtlichen Aspekte genauer, während Paul Frießem vom Fraunhofer-Institut für Sichere Informationstechnologie SIT näher auf die technischen Herausforderungen eingehen wird.

Natürlich bietet das Praxisforum auch Raum für Networking und ausführliche Gespräche mit ► den Referenten und Teilnehmern. Alle Mitglieder und Interessierten sind herzlich zu dieser Veranstaltung eingeladen. Weitere Informationen dazu gibt es im nächsten NIFIS advice. ❑

Corporate IAM Forum in Frankfurt

Vom 11. bis zum 13. November findet in Frankfurt am Main das Corporate Identity & Access Management Forum statt. IT-Sicherheitsverantwortliche, Infrastrukturarchitekten und Compliance-Verantwortliche treffen sich, um aktuelle Themen aus dem IAM-Umfeld zu diskutieren und um Projekterfahrungen auszutauschen.

Mathias Schabl von bident berichtet im Namen von NIFIS über Stolperfallen bei der IAM-Einführung. Dabei geht er unter anderem auf die Komplexität von IAM-Projekten, die User Acceptance und Awareness sowie die Definition von Rollen und Rechten näher ein.

Bei Anmeldungen bis zum 15. Oktober gibt es noch einen **Frühbucherrabatt**. ❑

Neue Mitglieder

„ActivIdentity entwickelt Softwarelösungen, mit deren Hilfe Individuen eine digitale Identität zugewiesen und verwaltet werden kann. Als einziger Anbieter am Markt können wir auf ein komplett eigen entwickeltes Produktspektrum verweisen. Wir freuen uns auf die Mitarbeit bei NIFIS, da wir einerseits davon ausgehen, dass wir unsere Kenntnisse sinnvoll in Diskussionen einbringen können. Andererseits können wir sicherlich auch Anforderungen anderer NIFIS-Teilnehmer und des Marktes aufnehmen und in unsere strategische Produktentwicklung einbeziehen."

Dirk Losse
Leiter Pre-Sales Consulting Central Europe
ActivIdentity GmbH

„dubois it-consulting gmbh unterstützt Kunden im Bereich Informations-Sicherheit und Zertifizierung. Die Ziele von NIFIS decken sich mit unseren Zielen und dem Geschäftszweck. Wir sind überzeugt, dass eine Gemeinschaft leichter und mehr für den Schutz vor bestehenden und neuen Gefahren tun kann. Hierzu möchten wir mit unserem Engagement und unserem Fachwissen beitragen. Außerdem sind für uns – so wie für andere Mitglieder auch – Informations-Austausch und Kontakte wichtige Elemente, um in unserer schnelllebigen, komplexen, teils hoch spezialisierten Geschäftswelt auf dem Laufenden zu sein und zu bleiben.“

Ingrid Dubois
Geschäftsführerin
dubois it-consulting gmbh

Service

Wissenschaftler stehen NIFIS Rede und Antwort

NIFIS legt großen Wert auf Wissenstransfer und Erfahrungsaustausch zwischen Wirtschaft, Politik und Wissenschaft. Die Universitätsprofessoren Prof. Dr. Klaus Merle (Mainz), Prof. Dr. Maximilian Herberger (Saarbrücken) und Prof. Dr. Dirk Heckmann (Passau) beraten NIFIS in Fragen rund um die Internet- und Informations-Sicherheit. NIFIS holt an dieser Stelle von den Experten regelmäßig Lösungsvorschläge zu aktuellen Herausforderungen und Antworten auf brisante Fragen ein.

Soeben ist der 17. Deutsche EDV-Gerichtstag zu Ende gegangen, an dem Sie auch in Ihrer Funktion als Vorsitzender des Beirats der Europäischen EDV-Akademie des Rechts teilgenommen haben. Welchen Stellenwert misst man E-Justice und in diesem Kontext der Informations-Sicherheit im elektronischen Rechtsverkehr bei?

Prof. Dr. Dirk Heckmann: E-Justice, die Modernisierung der Justiz mithilfe elektronischer Medien, wird immer wichtiger. Elektronische Registerauskünfte und eine – auch grenzüberschreitende – Registervernetzung, Online-Mahnverfahren oder die Klageerhebung über Justizportale sind längst Realität in Deutschland und Europa. Wie die Vorträge, aber auch die Begleitausstellung der Softwarehersteller und IT-Dienstleister in diesem Bereich gezeigt haben, sind dabei besonders IT-Sicherheit, Rechtssicherheit und Rechtsverbindlichkeit im Fokus neuer (Software-) Lösungen.

Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheits- und Internetrecht an der Universität Passau, wo er den bundesweit einzigartigen Studienschwerpunkt zum „IuK-Recht in der Verwaltung“ initiiert hat. Gemeinsam mit dem international renommierten Informatiker Hermann de Meer leitet er dort auch das interdisziplinäre Institut für IT-Sicherheit und Sicherheitsrecht.

Hervorzuheben sind hier die (rechts-) sichere Authentifizierung (zum Beispiel SAFE: Secure Access to Federated E-Justice), die beweiswerterhaltende Aufbewahrung von Dokumenten (viel Anklang fand das DMS des Saarländischen Justizministeriums) oder die rechtsverbindliche elektronische Aktenführung (im Einsatz etwa beim Bundespatentgericht). Von vielen Seiten ist zu hören, dass die notwendige Akzeptanz bei Richtern und Anwälten zur Umsetzung von E-Justice nur bei Gewährleistung von IT-Sicherheit erreicht werden kann. Die herausragende Stellung der Justiz als Garant von Sicherheit und Gerechtigkeit fordert besondere Anstrengungen, wie sie auch in der Arbeitsgruppe 9 auf dem IT-Gipfel der Bundesregierung am 20. November in Darmstadt diskutiert werden. Gleichsam als „kleiner Vorgipfel“ dient das E-Justice-Symposium, das an der Universität Passau am 29./30. Oktober veranstaltet wird. ❑

Expertenfrageecke

Zu viel Angst schadet am Ende auch

An dieser Stelle beantworten regelmäßig Experten Fragen, die NIFIS häufig erreichen, in dieser Ausgabe NIFIS-Vorstand Dr. Thomas Lapp. Sollten auch Sie eine Frage an unsere Experten haben, senden Sie diese einfach an newsletter@nifis.de.

Angstklauseln, vornehmer auch Disclaimer genannt, findet man sehr häufig am Ende von E-Mails. Nützen diese überhaupt, oder schaden sie eher?

Dr. Thomas Lapp: Unter Experten werden diese Texte bestenfalls für überflüssig und wirkungslos gehalten. Auch ohne juristische Kenntnisse muss man bei Klauseln am Ende einer E-Mail schmunzeln, die auf die Vertraulichkeit des gerade gelesenen Inhalts hinweisen und einem eventuell falschen Adressaten die Lektüre verbieten. Auch Klauseln, wonach die Kommunikation per E-Mail stets unverbindlich und nur die Kommunikation auf Papier verbindlich sein soll, müssen den Empfänger einer E-Mail im Jahr 2008 erstaunen.

Gerade die zuletzt genannte Klausel hat nunmehr einer Anwaltskanzlei eine böse Überraschung beschert. Der Mandant war im Rahmen einer rechtlichen Auseinandersetzung verpflichtet, gegenüber einem anderen Auskunft zu erteilen. Die Auskunft erteilte die Anwaltskanzlei für ihren Mandanten per E-Mail. In der E-Mail war nach der Signatur des Anwalts folgender Zusatz enthalten: „Aus Rechts- und Sicherheitsgründen ist die in dieser Mail gegebene Information nicht rechtsverbindlich. Eine rechtsverbindliche Bestätigung reichen wir Ihnen gerne auf Anforderung nach."

Nunmehr hat ein solcher Disclaimer dem Absender der E-Mail erstmals massiv geschadet. Das Landgericht Düsseldorf hat in einer Entscheidung vom 24.07.2008 festgestellt, dass man nicht einerseits erklären kann, E-Mail sei nicht rechtsverbindlich und sich andererseits auf die Verbindlichkeit der Erklärung berufen. Das Landgericht hat die Erklärung als unverbindlich eingestuft. Daran änderte auch der Nachsatz, man werde eine rechtsverbindliche Bestätigung auf Anforderung nachreichen, nichts. Heute ist die E-Mail im geschäftlichen Verkehr eine ganz normale Kommunikationsform. Klauseln, wonach diese Kommunikation nicht verbindlich sein soll, sind nicht mehr zeitgemäß. Wer, aus welchen Gründen auch immer, Papier für die bessere Basis von Kommunikation hält, sollte auch Papier verwenden und nicht auf Angstklauseln in E-Mails setzen. ❑

UTM – umfassende Netzwerksicherheit aus einer Hand

Was verbirgt sich eigentlich hinter dem Begriff Unified Threat Management (UTM), und welche Vor- und Nachteile bringt eine solche Lösung mit sich? Die Redaktion von NIFIS advice sprach mit Ralf Haubrich, Vice President Central Europe bei Astaro. Das NIFIS-Mitglied ist Anbieter von UTM- oder so genannten All-in-One-Lösungen und beschäftigt weltweit circa 180 Mitarbeiter. Im Marktsegment für UTM ist Astaro Marktführer in Deutschland und international die Nummer drei.

Herr Haubrich, Astaro wurde 2000 gegründet, der Begriff Unified Threat Management doch aber erst 2004 geschaffen …

… das stimmt, wir waren der Zeit etwas voraus: Astaro startete bereits 2000 mit All-in-One-Lösungen für IT-Sicherheit. Vier Jahre später definierte IDC erstmals UTM als eigenständigen Begriff. Unified Threat Management ist demnach ein All-in-One-Security-Konzept, das die Funktionen Intrusion Detection System (IDS), Antivirus, Firewall und Virtual Private Network (VPN) integriert. Heute sind die Infrastrukturen in Organisationen wesentlich komplexer geworden. Natürlich sind damit auch die Anforderungen an die IT-Sicherheit gestiegen und neue Produktmerkmale wie E-Mail-Verschlüsselung, Contentfilter, URL-Blocking oder Active-Directory-Anbindung werden benötigt. Da diese Entwicklung über die ursprüngliche Standarddefinition hinausgeht, sprechen wir heute von Extended Thread Management (XTM).

Das Grundkonzept von UTM besteht darin, mit einer zentral eingesetzten und verwalteten Lösung Sicherheit für das gesamte Netzwerk zu erlangen. Gibt es auch Komponenten, die nicht berücksichtigt werden?

Es gibt immer Grenzen. Eine UTM-Lösung stellt ein Gateway-Produkt dar, welches sich an der Schnittstelle zwischen Internet und Unternehmen befindet. Es kontrolliert alle ins Netzwerk ein- und ausgehenden Datenströme. Hiervon unberührt bleibt allerdings interner Traffic. Deshalb empfiehlt es sich, zusätzlich eine Desktop-Lösung für Antivirus oder die komplexe Analyse der gesamten Sicherheitsstruktur einzusetzen.

Für welche Unternehmen ist ein UTM-Produkt besonders interessant?

Grundsätzlich für alle Organisationen. Aber besonders kleine und mittelständische Unternehmen mit zehn bis 1.000 Nutzern oder auch Unternehmen, die weder eine dedizierte Sicherheitsabteilung haben noch die Manpower und auch nicht das Know-how besitzen, um sich um Sicherheit zu kümmern, profitieren von UTM. In großen Unternehmen mit 300.000 Nutzern gibt es eine spezielle Sicherheitsabteilung und auch oft besondere Anforderungen.

Viele Unternehmen setzen bereits eine Firewall und Virenschutz ein. Müssen sie ihre bisherigen Produkte abschaffen und in eine komplett neue Lösung investieren?

Für ein Unternehmen, das bislang keinerlei IT-Security-Vorkehrungen getroffen hat, stellt ein UTM-Produkt die optimale Lösung dar. Befindet sich aber beispielsweise schon eine Firewall im Einsatz, kann diese natürlich weiterhin genutzt und die UTM-Lösung als reiner Contentfilter für Mail und Web angeschafft werden. Wichtig ist die Analyse der bestehenden Infrastruktur im Vorfeld. So wird sichergestellt, dass das UTM-Produkt effizient in Betrieb genommen wird und ermittelt, ob bestehende Sicherheitselemente entfernt oder ein Mehrstufenkonzept aufgebaut werden sollte.

Können Unternehmen eine UTM-Lösung selbst installieren und warten?

Ralf Haubrich,
Vice President
Central Europe bei Astaro

Ja, wenn sie über ausreichend Security-Know-how im Unternehmen verfügen. Bei UTM-Lösungen handelt es sich um ein umfassendes und abgeschlossenes IT-Sicherheitskonzept. Die Installation einzelner Applikationen entfällt damit. Administratoren sind in der Lage, nahezu alle Sicherheitsfunktionen innerhalb kürzester Zeit zu verstehen und die UTM-Appliance schnell ins Netzwerk zu integrieren.

Zeitgemäße Produkte haben eine webbasierte, grafische Benutzeroberfläche, die sehr einfach zu bedienen ist. Trotzdem empfehle ich, qualifizierte Partner oder ein Systemhaus vor Ort zu Rate zu ziehen, um die bestehende Infrastruktur zu analysieren und um bei der Installation die Verfügbarkeit der Systeme zu gewährleisten.

Kommen auch die Endanwender mit der Lösung in Kontakt?

Größtenteils wird das Produkt natürlich vom Administrator verwaltet. Es gibt allerdings auch UTM-Produkte, die den Mitarbeitern so genannte Quarantäne Reports zur Verfügung stellen. Mithilfe dieser Berichte kann der User einsehen, welche E-Mail in Quarantäne gestellt, oder was als Spam geblockt wurde. Somit lässt sich auch eine persönliche Whitelist erstellen oder aber überprüfen, wo eine bestimmte E-Mail im System gelandet ist. Ansonsten bleibt der Endanwender von dem System gänzlich unberührt.

Warum empfiehlt sich der Einsatz einer UTM-Lösung im Unternehmen?

Es wird heute eine Vielzahl an Sicherheitssystemen angeboten. Viele Unternehmen haben aber nicht die Zeit und das Know-how, diese Systeme zu pflegen. Jedes einzelne System wie Firewall, VPN oder IDS hat eine andere Administrationsoberfläche, einen eigenen Update-Mechanismus und muss gezielt überwacht werden. ►

Hinzu kommen kostspielige Schulungen für den IT-Administrator. Ein UTM-Produkt bietet alle Funktionalitäten aus einer Hand – mit nur einer Oberfläche und einem Update-Mechanismus, der stets neueste Pattern zur Verfügung stellt. Bei intelligenten Lösungen funktioniert das Einspielen von Viren-Pattern oder IDS-Updates in das System automatisch, ohne dass der Administrator eingreifen muss.

Große Updates mit neuen Sicherheitsanforderungen oder neuen Features werden durch den Hersteller abgelegt und der Administrator benachrichtigt, sodass dieser im Rahmen seiner Wartungsfenster das System neu aufsetzen kann.

Wenn mein Spamfilter ausfällt, habe ich vorübergehend keine Spamkontrolle. Aber was passiert, wenn die UTM-Lösung ausfällt?

Um dieser Problematik Herr zu werden, gibt es beispielsweise Hochverfügbarkeitslösungen bis hin zu patentierten Clusterlösungen. In diesem Falle sind zwei Systeme aneinander gekoppelt. Im Falle eines Systemausfalls übernimmt das andere in weniger als zwei Sekunden die Kontrolle des Netzwerks. ►

Die Investition in ein solches System lohnt sich dennoch: Denn – wird nur ein Gateway zur Absicherung des Netzwerks eingesetzt, so ist bei Systemausfall keinerlei Kommunikation mehr von und zum Internet mit allen verbundenen Diensten möglich. Das ist in der heutigen Zeit äußerst geschäftskritisch.

Sind mit UTM auch Nachteile verbunden?

Nein.

Warum sind Sie NIFIS-Mitglied geworden?

Als Experte für IT-Sicherheit war es für uns ganz selbstverständlich eine Organisation wie NIFIS zu unterstützen. Zukünftig planen wir verstärkt die aktive Mitarbeit in einigen Expertenforen. Denn NIFIS übernimmt als Selbsthilfeorganisation eine Vorreiterrolle zum Schutz gegen die Gefahren des Internets. In dieser Position ist sie in der Lage, unabhängig und kompetent praxisnahe Hilfestellung für Unternehmen anzubieten, Der besondere Erfolg der Organisation liegt hierbei in der interdisziplinären Kompetenzbündelung aller unterschiedlichen NIFIS-Mitglieder.

Vielen Dank für das Gespräch! ❑

Sicherheitsupdate

Schutz geschäftskritischer Daten

Rechenzentren haben sich für viele Unternehmen zur Schaltzentrale entwickelt, ohne die sich der reguläre Geschäftsbetrieb nicht aufrechterhalten lässt. Dem Schutz des Rechenzentrums, der dort laufenden Applikationen und den geschäftskritischen Daten kommt somit eine zentrale Bedeutung zu.

So manchem Entscheider ist gar nicht bewusst, dass er je nach Rechtsform und Art des Unternehmens mehr oder minder strengen Gesetzen und Verordnungen unterworfen ist, die dazu verpflichten, dessen Fortbestand auch im Fall von Naturereignissen oder Terrorakten zu gewährleisten. Durch die Eigenkapitalvereinbarung „Basel II" und die Standards zur Vergabe von Krediten kommt es verstärkt darauf an, Risiken des IT-Betriebs einschätzen zu können. Die Firmen-IT ist häufig eng mit kritischen Bereichen wie Buchhaltung, Warenwirtschaft oder Produktionssteuerung verzahnt oder stellt sogar die Grundlage des Geschäftsmodells dar. Daher müssen die Sicherheit des Rechenzentrums (RZ) im Allgemeinen und die häufig unterschätzte physikalische Absicherung im Besonderen in den Mittelpunkt des Interesses rücken. Dies gilt nicht nur für große Konzerne, Banken und Versicherungen, sondern zunehmend auch für Mittelständler und ist unabhängig davon, ob das Unternehmen ein eigenes Rechenzentrum betreibt oder RZ-Dienstleistungen über einen Provider einkauft.

Sicherheit beginnt mit der Planung

Um herauszufinden, welche physikalische Sicherheit sie brauchen, sollten Unternehmen methodisch vorgehen und mindestens einen Verantwortlichen für das Thema benennen. Auf diese Weise lässt sich mit vertretbarem Aufwand ein auf die jeweilige Organisation zugeschnittenes Sicherheitskonzept entwickeln.

Am Anfang der Planung sollte in jedem Fall die Anforderungsanalyse stehen. Hierbei handelt es sich um eine Risikoabschätzung im Hinblick auf mögliche Gefahren, die sich beispielsweise durch die Art des Geschäftsbetriebs, den Standort des RZ und weitere Faktoren ergeben. Als Nächstes gilt es, die erforderlichen Schutzmaßnahmen samt technischer Umsetzung zu ermitteln. Da sich die Parameter im Lauf der Zeit ändern, sollte alles schriftlich dokumentiert und im Sinn eines Qualitäts-Managements regelmäßig überprüft werden. Nur so kann Sicherheit dauerhaft aufrechterhalten werden. ►

IMMER UP TO DATE

Um Sie effizient zu schützen, bietet NIFIS auf ihrer Website tagesaktuelle Warnhinweise zu Bedrohungen im Internet. Alle aufgeführten Meldungen sind CERT-geprüft (Computer Emergency Response Team) und haben ein hohes Schadens- und Risikopotenzial. Links zu weiterführenden Informationen unterstützen Sie beim schnellen Beseitigen der Sicherheitsbedrohung.

„Wird der Betrieb eines eigenen RZ in Betracht gezogen, ist es wichtig, eine Vision zu entwickeln und diese während der gesamten Planung und Umsetzung im Auge zu behalten", rät Peter Heinemann, der als Senior Consultant beim Frankfurter Rechenzentrumsbetreiber Interxion tätig ist. „Essenziell ist zudem, nicht die technisch perfekte Detaillösung anzustreben, sondern auf eine optimale Abstimmung der einzelnen Elemente zu achten." Anhaltspunkte, welche Anforderungen bei der physikalischen Sicherheit zu berücksichtigen sind, liefern beispielsweise das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI), der BSI-Standard 100-2 oder die ISO-Norm 27001:2005. Bei Bedarf kann sich ein RZ-Betreiber beispielsweise vom TÜV gemäß ISO 27001 zertifizieren lassen, um den eigenen Qualitätsstandard zu dokumentieren.

Gefahren erkennen

Schon der Standort macht ein Rechenzentrum sicher oder unsicher. So kann ein nahe gelegener Bach bereits ein Überschwemmungsrisiko bedeuten. Dasselbe gilt für nahe Industrieanlagen, etwa der chemischen Industrie.

Ist der geeignete Standort identifiziert, ist es notwendig, sich dem Thema Zutrittsschutz zu widmen. Sofern sich das Rechenzentrum nicht ohnehin auf einem geschützten Werksgelände befindet, muss unbefugter Zutritt zum Gelände eigens verhindert werden. Dazu können kameraüberwachte Zäune ebenso dienen wie Sicherheitspersonal, das in regelmäßigen Abständen Kontrollgänge absolviert. Auch einbruchssichere Türen und Fenster sowie weitere Überwachungs- und Alarmeinrichtungen können sich als sinnvoll erweisen.

Ohne Zutrittskontrolle keine Sicherheit

In einem nächsten Schritt gilt es, zu überlegen, wer Zutritt zum Gebäude erhalten soll – und den Zugang entsprechend abzusichern. So empfiehlt es sich, einen Empfangsbereich einzurichten, der etwa durch Vereinzelungsschleusen von den technischen Bereichen abgetrennt ist. Namen und Anwesenheitszeiten von Besuchern sollten vom Sicherheitspersonal dokumentiert werden. Zudem ist der Zutritt zu den Technikräumen sowie zu den einzelnen Schränken über geeignete Zutrittssysteme nochmals separat abzusichern. Dies gilt insbesondere, wenn RZ-Dienstleistungen über einen Provider in Anspruch genommen werden. Häufig bieten diese separat abschließbare, kundenindividuelle Cages an, die ausschließlich für das Equipment eines Kunden reserviert sind.

Bewegungsmelder sowie zusätzliche Kamerasysteme unterstützen das Sicherheitspersonal dabei, Missbrauch, Manipulationen oder Diebstahl vorzubeugen. Für Interxion-Berater Heinemann stellt die Zutrittsregulierung sogar den wichtigsten Aspekt der physikalischen Sicherheit dar: „Als Rechenzentrumsbetreiber ist es für uns essentiell, die volle Kontrolle darüber zu behalten, welche Personen unsere Anlagen betreten und wieder verlassen. Dies gilt speziell für Betriebsfremde."

Gefahren drohen jedoch nicht nur von außen, sondern lauern auch im Inneren des Rechenzentrums. Ein wichtiges Thema ist hier der Brandschutz. In jedem Fall sinnvoll ist eine Unterteilung des RZ in verschiedene Brandschutzabschnitte, wobei durch bauliche Maßnahmen vermieden wird, dass ein Brand von einem Bereich auf einen anderen übergreift. Durch Cluster-Systeme und andere Redundanzen kann so der IT-Betrieb selbst dann aufrechterhalten werden, wenn ein Raum brennt. Auch Sicherheitszonen im Sinne einer Haus-im-Haus- oder Raum-in-Raum-Lösung, die von der Industrie angeboten werden, können sich dabei als sinnvoll erweisen. Systeme, die sich in solchen Schutzräumen befinden, sind über mehrere Stunden sicher vor Bränden, die sich außerhalb der Sicherheitszelle ereignen. Um einen Brand rechtzeitig erkennen zu können, ist zudem die Installation von Sensoren und Detektoren sinnvoll, die auf Rauch- und Schwelgase sowie einen ungewöhnlichen Temperaturanstieg reagieren.

Kühlung schützt vor Feuer

Überhitzung kann zu Systemausfällen oder gar Bränden führen. Deshalb ist die ausreichende Kühlung der empfindlichen Gerätschaften Pflicht. Dabei ist zu überlegen, ob eine Kühlung über den Doppelboden ausreicht oder die spezielle Kühlung jedes einzelnen Schrankes über ein High-Density-Klimagerät ratsam ist. Besonders Blade-Systeme neigen zur Bildung von „Hotspots" im Server-Schrank. (weiterlesen)

Redaktion COMPUTERWOCHE

Weitere interessante Sicherheits-Nachrichten des NIFIS-Kooperationspartners Computerwoche finden Sie hier. ❑

IMPRESSUM

Herausgeber
NIFIS e.V.
Weismüllerstraße 21
60314 Frankfurt
Tel.: 0 69 / 40 80 93 70
Fax: 0 69 / 40 14 71 59
E-Mail: newsletter@nifis.de
Internet: http://www.nifis.de
Peter Knapp (V.i.S.d.P.)

Redaktion
FRESH INFO +++
Nicole Chemnitz (CvD)
http://www.fresh-info.de